

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/016686

International filing date: 05 September 2005 (05.09.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-258186
Filing date: 06 September 2004 (06.09.2004)

Date of receipt at the International Bureau: 20 October 2005 (20.10.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 4 年 9 月 6 日

出 願 番 号
Application Number: 特 願 2 0 0 4 - 2 5 8 1 8 6

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

J P 2 0 0 4 - 2 5 8 1 8 6

出 願 人
Applicant(s): ソニー株式会社

2 0 0 5 年 9 月 2 1 日

特許庁長官
Commissioner,
Japan Patent Office

中 嶋



【書類名】	特許願
【整理番号】	0390770004
【特記事項】	特許法第36条の2第1項の規定による特許出願
【提出日】	平成16年 9月 6日
【あて先】	特許庁長官殿
【国際特許分類】	G06F 7/58
【発明者】	
【住所又は居所】	東京都品川区北品川6丁目7番35号 ソニー株式会社内
【氏名】	ミオドラッグ ミハイエビッチ
【発明者】	
【住所又は居所】	東京都品川区北品川6丁目7番35号 ソニー株式会社内
【氏名】	阿部 譲司
【特許出願人】	
【識別番号】	000002185
【氏名又は名称】	ソニー株式会社
【代表者】	安藤 国威
【連絡先】	知的財産部 03-5435-3909
【手数料の表示】	
【予納台帳番号】	005094
【納付金額】	26,000円
【提出物件の目録】	
【物件名】	外国語特許請求の範囲 1
【物件名】	外国語明細書 1
【物件名】	外国語図面 1
【物件名】	外国語要約書 1

【書類名】	翻訳文提出書
【整理番号】	0390770004
【提出日】	平成16年11月 8日
【あて先】	特許庁長官 殿
【出願の表示】	
【出願番号】	特願2004-258186
【特許出願人】	
【識別番号】	000002185
【氏名又は名称】	ソニー株式会社
【代表者】	安藤 国威
【確認事項】	本書に添付した翻訳文は、外国語書面出願の願書に添付して提出した外国語明細書、外国語図面及び外国語要約書に記載した事項を過不足なく適正な日本語に翻訳したものである。
【提出物件の目録】	
【物件名】	外国語特許請求の範囲の翻訳文 1
【物件名】	外国語明細書の翻訳文 1
【物件名】	外国語図面の翻訳文 1
【物件名】	外国語要約書の翻訳文 1

【書類名】 特許請求の範囲

【請求項 1】

疑似乱数シーケンスを生成する装置において、
より高いランダム性を有する第 1 のシーケンスを生成する第 1 のタイプのセルオートマトンと、
周期について予め定めた下限を有する第 2 のシーケンスを生成する第 2 のタイプのセルオートマトンと、
前記第 1 のシーケンスおよび前記第 2 のシーケンスに対してビット毎の $\text{mod } 2$ の和を求める加算器とを備えること
を特徴とする装置。

【請求項 2】

前記第 1 のタイプのセルオートマトンは、二次元セルオートマトンであり、
前記第 2 のタイプのセルオートマトンは、 2×1 セルオートマトンであり、
前記加算器の合計結果は、前記疑似乱数シーケンスとして出力されること
を特徴とする請求項 1 に記載の装置。

【請求項 3】

対応するセル制御ワードおよび／またはルール制御ワードに基づいて状態が計算され得るセルを有し、第 3 のシーケンスを生成する第 3 のタイプのセルオートマトンをさらに備え、
前記セル制御ワードは、前記第 2 のタイプのセルオートマトンにより生成され、
前記ルール制御ワードは、前記第 1 のタイプのセルオートマトンにより生成され、
前記加算器は、前記第 1、第 2 および第 3 のシーケンスのビット毎の $\text{mod } 2$ の和を得ること
を特徴とする請求項 1 に記載の装置。

【請求項 4】

前記加算器の合計結果は、前記疑似乱数シーケンスとして出力されること
を特徴とする請求項 3 に記載の装置。

【請求項 5】

前記加算器からの合計結果に対し非線形マッピングを行なうブロックと、
前記非線形マッピングの結果に対して不均一な間引きを行なうブロックとをさらに備え

前記間引き結果が前記疑似乱数シーケンスとして出力されること
を特徴とする請求項 2 または請求項 4 に記載の装置。

【請求項 6】

前記ブロックの各々が、少なくとも 1 つの非線形関数を含むこと
を特徴とする請求項 5 に記載の装置。

【請求項 7】

前記非線形マッピングを行なうブロックは、ラテン方格 (Latin square) に基づいた非線形マッピング用の参照テーブルを少なくとも 1 つ含むこと
を特徴とする請求項 5 に記載の装置。

【請求項 8】

暗号処理を行なう装置において、
疑似乱数シーケンスを用いてデータを暗号化する暗号プロセッサと、
前記疑似乱数シーケンスを生成する疑似乱数シーケンス生成器とを備え、
前記疑似乱数生成器は、請求項 1 乃至 7 のいずれかに記載の装置を含んで構成されること
を特徴とする装置。

【請求項 9】

セルオートマトンを用いて疑似乱数シーケンスを生成する方法において、
より高いランダム性を有する第 1 のシーケンスを生成するステップと、

周期について予め定めた下限を有する第2のシーケンスの生成するステップと、
前記第1のシーケンスおよび前記第2のシーケンスのビット毎の $\text{mod } 2$ の和を得るステップとを備えていること
を特徴とする方法。

【請求項10】

セルオートマトンを用いて疑似乱数シーケンスを生成する方法をコンピュータに実行させるコンピュータプログラムにおいて、

前記方法は、

より高いランダム性を有する第1のシーケンスを生成するステップと、

周期について予め定めた下限を有する第2のシーケンスの生成するステップと、

前記第1のシーケンスおよび前記第2のシーケンスのビット毎の $\text{mod } 2$ の和を得るステップとを備えていること

を特徴とするコンピュータプログラム。

【請求項11】

セルオートマトンを用いて疑似乱数シーケンスを生成する方法をコンピュータに実行させるコンピュータプログラムを格納する記録媒体において、

前記方法は、

より高いランダム性を有する第1のシーケンスを生成するステップと、

周期について予め定めた下限を有する第2のシーケンスの生成するステップと、

前記第1のシーケンスおよび前記第2のシーケンスのビット毎の $\text{mod } 2$ の和を得るステップとを備えていること

を特徴とする記録媒体。

【書類名】明細書

【発明の名称】セルオートマトンに基づく、制御可能な周期を有する疑似乱数シーケンスの生成方法および装置

【技術分野】

【0001】

本発明は、コンパクトな有限状態機械を用いて、制御可能な周期を有する疑似乱数シーケンスを生成する方法および装置に関する。

【背景技術】

【0002】

近年、セルオートマトンの利用に基づいた、極めて良好な統計特性を備えた疑似乱数シーケンスの生成方法が多く報告されている。例えば、非特許文献1は、高品質乱数を生成する二次元のセルオートマトンを開示している。以下に、典型的な二次元のセルオートマトン(2D-CA)について説明する。

【0003】

セルオートマトン(CA)は、空間と時間が互いに離散している動的システムである。セルオートマトンは、局所近傍則(local interaction rule)に従ったセルアレイ(cellular array)から構成される。セルの各々は、離散した時間ステップで同期更新されるもので、取りうる有限数の状態のうちの1つとなることができる。ここでは、セルの状態が $s_i \in \{0, 1\}$ となるブーリアンオートマトンだけを考慮するものとする。次のステップにおけるセルの状態は、周辺近傍セルの現在の状態によって決定される。

【0004】

セルアレイ(グリッド)は d 次元で、実用に際しては $d=1, 2, 3$ が使用される。本明細書のこのセクションでは、 $d=2$ 、つまり二次元のグリッドが考慮される。

【0005】

各セルに含まれているルールは、本質的に有限状態機械ルールであって、通常はルール・テーブル(遷移関数としても知られている)の形で特定されており、状態に関して可能性のある近傍配置すべてについてのエントリを含んでいる。1つのセルのセル近傍構造(neighborhood)は、それ自体および周囲の(隣接する)セルからなる。一次元のCAについては、セルは、いずれか一方の側で r のローカルな近傍(セル)に接続される。ここで、 r は半径と呼ばれるので、各セルは $2r+1$ の近傍を有する。

【0006】

二次元CA(2D-CA)については、2つのタイプのセル近傍が通常考慮される。これらは次のとおりである：その直近の非対角線の4つの近傍(フォンノイマンの近傍としても知られている)及び当該セルからなる5つのセルと、その周囲の8つの近傍及び当該セルからなる9つのセル(ムーアの近傍としても知られている)とがある。

【0007】

有限のサイズのグリッドを考慮する場合、周期的な境界条件が良く使われ、一次元の場合には円形状グリッド(circular)に、二次元の場合には環状体(toroidal)のものとなる。また、固定あるいはヌル(null)の境界条件も使用することもできる。この場合、グリッドは固定した状態あるいは0(零)の状態にあるセルからなる外部層で囲まれる。後者の場合、通常、ハードウェアで実施するのが容易である。

【0008】

不均一の(あるいは異質)セルオートマトンは、均質なものと同じ方法で機能するが、唯一の相違点は、セルルールをすべてのセルに対して同一とする必要がないということである。不均一のCAも、均質のものと同様に、基本的で有利な特性、即ち単純性、並行性(parallelism)およびローカル性を共有する。

【0009】

2D-CAについての適切な背景的考察は、例えば非特許文献2に開示されている。

【0010】

【非特許文献1】M. Tomassini, M. Sipperand, M. Perrenoud, "On the generation

of high-quality random number by two-dimensional cellular automata"「二次元のセルオートマトンによる高品質乱数の生成について」, IEEE Trans. Computers, vol. 49, pp. 1146-1151, Oct. 2000

【0011】

【非特許文献2】P. P. Chaudhuri, D. R. Chaudhuri, S. Nandi and, S. Chattopadhyay, "Additive Cellular Automata: Theory and Applications"「加法的セルオートマトン：理論および応用」, New York, IEEE Press, 1997.

【非特許文献3】S. Wolfram, "Cryptography with Cellular Automata"「セルオートマトンによる暗号法」, Advances in cryptology - CRYPTO85, Lecture Notes in Computer Science, vol. 218, pp. 429-432, 1985

【非特許文献4】K. Cattell, S. Zhang, M. Serra and, J. C. Muzio, "2-by-n hybrid cellular automata with regular configuration: Theory and application"「規則的な配置を備えた $2 \times n$ ハイブリッドセルオートマトン：理論および応用」, IEEE Trans. Computers, vol. 48, pp. 285-295, March 1999

【非特許文献5】A. Klimov and A. Shamir, "Cryptographic applications of T-functions"「T関数の暗号の応用」, SAC'2003, pre-print 15 pages, August 2003, (to appear in Lecture Notes in Computer Science)

【非特許文献6】S.-U. Guan and S. Zhang, "An evolutionary approach to the design of controllable cellular automata: structure for random number generation"「制御可能なセルオートマトン設計への進化したアプローチ：乱数発生用構造」, IEEE Trans. Evolutionary Computation, vol. 7, pp. 23-36, Feb. 2003.

【非特許文献7】P. D. Hortensius, R. D. McLeod, W. Pries, D. M. Miller and H. C. Card, "Cellular automata-base pseudorandom number generators for built-in self-test"「セルオートマトンに基づく、ビルトイン・セルフテスト用の疑似乱数生成器」, IEEE Transactions on Computer-Aided Design, vol. 8, pp. 842-859, August 1989.

【非特許文献8】M. Mihaljevic, M. P. C. Fossorier and H. Imai, "Fast correlation attack algorithm with the list decoding and an application"「リスト符号解読およびアプリケーションを備えた高速相関性攻撃アルゴリズム」, FSE2001, Lecture Notes in Computer Science, vol. 2355, pp. 196-210, 2002.

【非特許文献9】N. T. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback"「線形フィードバックによるストリーム暗号への代数的攻撃」, EURO-CRYPT2003, Lecture Notes in Computer Science, vol. 2656, pp. 345-359, 2003.

【非特許文献10】M. Mihaljevic and H. Imai, "A family of fast keystream generators based on programmable linear cellular automata over GF(q) and time variant table"「GF(q)および時間変化テーブルに対するプログラム可能な線形のセルオートマトンに基づく、高速キーストリーム生成器のファミリ」, IEICE Transactions on Fundamentals, vol. E82-A, pp. 32-39, Jan. 1999.

【非特許文献11】G. Marsaglia, "Diehard"「ダイハード」(1998). <http://jstat.fsu.edu/geo/diehard.htm>.

【非特許文献12】A. K. Das, A. Ganguly, A. Dasgupta, S. Bhawmik, and P. Pal Chaudhuri, "Efficient characterization of cellular automata", 「セルオートマトンの効率的な特性」, IEE Proc. Pt. E, vol. 137, pp. 81-87, Jan. 1990.

【非特許文献13】K. Cattell and J. C. Muzio, "Synthesis of one-dimensional linear hybrid cellular automata"「一次元線形ハイブリッド・セルオートマトンの合成」, IEEE Trans. Computer-Aided Design, vol. 15, pp. 325-335, March 1996.

【非特許文献14】S. Nandi, B. K. Kar and P. Pal Chaudhuri, "Theory and applications of cellular automata in cryptography"「暗号法でのセルオートマトンの理論および応用」, IEEE Trans. Comput., vol. 43, pp. 1346-1357, Dec. 1994.

【非特許文献15】W. Meier and O. Staffelbach, "Analysis of pseudo random sequences generated by cellular automata"「セルオートマトンによって生成された疑似乱数シーケンスの分析」, Advances in Cryptology - EUROCRYPT 91, Lecture Notes in Computer Science, vol. 547, pp. 186-189, 1992.

【非特許文献16】C. K. Koc and A.M. Apohan, "Inversion of cellular automata iterations"「セルオートマトン反復の転位」, IEE Proc. Comput. Digit. Tech., vol. 144, pp. 279-284, 1997.

【非特許文献17】M. Mihaljevic, "An improved key stream generator based on the programmable cellular automata"「プログラム可能なセルオートマトンに基づいた、改良キーストリーム生成器」, ICICS'97, Lecture Notes in Computer Science, vol. 1334, pp. 181-191, 1997.

【非特許文献18】M. Mihaljevic, "Security examination of a cellular automata based pseudorandom bit generator using an algebraic replica approach"「代数的複製アプローチを使用する、セルオートマトン・ベースの疑似乱数ビット生成器のセキュリティ試験」, AAEC12, Lecture Notes in Computer Science, vol. 1255, pp. 250-262, 1997.

【非特許文献19】S.R. Blackburn, S. Murphy and K.G. Peterson, "Comments on 'Theory and Applications of Cellular Automata in Cryptography'"「『暗号法でのセルオートマトンの理論および応用』に関するコメント」, IEEE Trans. Comput., vol. 46, pp. 637-638, May 1997.

【非特許文献20】M. Mihaljevic, "Security examination of a cellular automata based pseudorandom bit generator using an algebraic replica approach"「代数的複製アプローチを使用する、セルオートマトン・ベースの疑似乱数ビット生成器のセキュリティ試験」, AAEC12, Lecture Notes in Computer Science, vol. 1255, pp. 250-262, 1997.

【非特許文献21】A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography (応用暗号法ハンドブック), Boc. Roton: CRC Press, 1997.

【発明の開示】

【発明が解決しようとする課題】

【0012】

しかしながら、上述の提案の主な欠点は、生成された疑似乱数シーケンスの周期に関して保証がないことである。従って、上述したような望ましい統計特性のランダム性を備えた、最大または実質的に最大周期のシーケンスを生成するための方法と装置を提供することが望ましい。

【0013】

本発明は上記を考慮してなされている。本発明の目的は、制御可能な周期を有する、所望の疑似乱数シーケンスを生成する方法および／またはコンパクトな装置を提供することにある。

【課題を解決するための手段】

【0014】

本発明の一実施形態によれば、疑似乱数シーケンス生成装置が提供される。本装置は、より高いランダム性を有する第1のシーケンスを生成する第1のタイプのセルオートマトンと、周期について予め定めた下限を有する第2のシーケンスを生成する第2のタイプのセルオートマトンと、前記第1のシーケンスおよび前記第2のシーケンスに対してビット毎のmod 2の和を求める加算器とを備えることを特徴とする。

【0015】

本実施形態による装置では、前記第1のタイプのセルオートマトンは、二次元セルオートマトンであってもよく、前記第2のタイプのセルオートマトンは、2×Lセルオートマトンであってもよい。また、前記加算器からの合計結果は、疑似乱数シーケンスとして出

力され得る。

【0016】

本発明の他の実施形態によれば、上述した装置において、第3のシーケンスを生成するための第3のタイプのセルオートマトンをさらに備えていてもよい。前記第3のタイプのセルオートマトンは、対応するセル制御ワードおよび／またはルール制御ワードに基づいて、状態が計算され得るセルを有する。本実施形態では、前記セル制御ワードは、前記第2のタイプのセルオートマトンによって生成され、前記ルール制御ワードは、前記第1のタイプのセルオートマトンによって生成され、前記加算器は、前記第1、第2および第3のシーケンスのビット毎の $\text{mod } 2$ の和を得る。

【0017】

本発明のさらに他の実施形態によれば、上述した装置において、前記加算器からの合計結果に非線形マッピングを行なうブロックと、該非線形マッピングの結果について不均一な間引きを行なうブロックとをさらに備え、前記間引き結果が前記疑似乱数シーケンスとして出力されてもよい。本装置では、前記ブロックの各々が、少なくとも1つの非線形関数を含んでいてもよい。あるいは、前記非線形マッピングを行なうブロックは、ラテン方格 (Latin square) に基づいた非線形マッピング用参照テーブルを少なくとも1つ含んでもよい。

【0018】

本発明の他の実施形態によれば、暗号処理を行なう装置が提供される。本装置は、疑似乱数シーケンスを用いてデータを暗号化する暗号プロセッサと、前記疑似乱数シーケンスを生成する疑似乱数シーケンス生成器とを含むことを特徴とする。本実施形態では、前記疑似乱数生成器は、上記実施形態のうちの任意の1つによる装置を含むように構成される。

【0019】

本発明の他の実施形態によれば、セルオートマトンを用いて疑似乱数シーケンスを生成する方法、または該方法をコンピュータに実行させるコンピュータプログラム、または該コンピュータプログラムを格納する記録媒体が提供される。前記方法は、より高いランダム性を有する第1のシーケンスを生成するステップと、周期について予め定めた下限を有する第2のシーケンスの生成するステップと、前記第1のシーケンスおよび前記第2のシーケンスのビット毎の $\text{mod } 2$ の和を得るステップとを備えている。

【発明の効果】

【0020】

本発明によれば、制御可能な周期を有する所望の疑似乱数シーケンスの生成方法および／またはコンパクトな装置が提供される。

【発明を実施するための最良の形態】

【0021】

第1の実施形態：

本発明の第1の実施形態によれば、コンパクトな有限状態機械 (finite state machine) を用いて、制御可能な周期を有する疑似乱数シーケンスを生成する方法および装置が提供される。本実施形態による装置は、セルオートマトンの2つの異なるクラスに基づくものである。本装置および本方法は、フレキシブルであり、空間複雑度とシーケンス周期の下限の間のトレードオフ (trade-off) についての好機を与えるものである。

【0022】

本発明の第1の実施形態について説明する前に、セルオートマトンに関する基礎技術のうち、本実施形態で使用されるいくつかの技術について、添付図面を参照して説明する。

【0023】

基本的なバイナリ・セルオートマトン (Basic Binary Cellular Automata)：

一次元のバイナリ・セルオートマトン (CA) は、直列接続された、0あるいは1の値をとる L 個のセルアレイと、 q 個の変数を有するブール関数 $f(x)$ の値とから構成される。セル x_i の値は、 $i=1, 2, \dots, L$ について、 $x'_i = f(x)$ として、離散

時間ステップでこの関数を使用して、パラレルに（同期して）更新される。境界条件は、通常、指標値モジュール L をとることにより処理される。パラメータ q は、通常、奇数の整数（つまり $q = 2r + 1$ ）であり、ここで r は、関数 $f(x)$ の半径としはしば呼ばれる。 i 番目のセルの新しい値は、 i 番目のセルの値、および i 番目のセルの左右 r 個近傍のセルの値を使用して計算される。

【0024】

各々が 0 または 1 の値をとる L 個のセルがあるので、 2^L 個の可能な状態ベクトルがある。 S_k で、時間ステップ k での状態ベクトルを表わすものとする。初期状態ベクトル S_0 からスタートして、セルオートマトンは、時間ステップ $k = 1; 2; 3; \dots$ など、状態 S_1, S_2, S_3 などに移る。状態ベクトル S_k は、 k が進むにつれて、 L ビットのバイナリ・ベクトルの群（セット）から値を取り、状態マシンは結果として循環する。つまり、以前（ $S_k = S_{k+P}$ ）に到達した状態 S_{k+P} に達する。この周期 P は、初期状態、更新機能およびセル数の関数である。

【0025】

$q = 3$ を有する CA については、各離散時間ステップ t （時計サイクル）で i 番目のセルの展開は、 $(i-1)$ 番目、 (i) 番目、 $(i+1)$ 番目セルの現在の状態の関数として表わすことができる。

【0026】

【数1】

$$x_i(t+1) = \{ f(x_{i-1}(t), x_i(t), x_{i+1}(t)) \} \quad \dots (1)$$

【0027】

f は CA に関連した組合せ論理 (combinatorial logic) とも呼ばれる。組合せ論理は、それぞれ次の状態に展開するために更新ルールを表わす。

【0028】

セルの次の状態関数が真理値表 (truth table) の形で表現される場合、真理値表中の出力カラムの 10 進の等価は、従来通りに CA ルール番号と呼ばれる。非特許文献 3 の中で提案され考慮したルール 30 と呼ばれる非線形ルールは、下記によって更新を実現する：

【0029】

【数2】

$$x_i(t+1) = x_{i-1}(t) \text{ XOR } [x_i(t) \text{ OR } x_{i+1}(t)] \quad \dots (2)$$

【0030】

特に興味深いのは $GF(2)$ に関する 2 つの線形ルールである。これらは、ルール 90 およびルール 150 としてそれぞれ知られている。ルール 90 では、以下の組合せ論理に従って、現在から次の状態までの展開（更新）を指定する：

【0031】

【数3】

$$x_i(t+1) = x_{i-1}(t) \oplus x_{i+1}(t) \quad \dots (3)$$

【0032】

ここで、丸に十字の記号（以下「 \oplus 」と略す）は XOR 演算を示す。なお、ルール 90 が適用される場合、 i 番目のセルの次の状態が、その左右の近傍の現在の状態に依存する。同様に、ルール 150 用の組合せ論理は、以下により与えられる：

【0033】

【数4】

$$x_i(t+1) = x_{i-1}(t) \oplus x_i(t) \oplus x_{i+1}(t) \quad \dots (4)$$

【0034】

すなわち、 i 番目のセルの次の状態は、その左右の近傍の現在の状態およびさらにそれ自身の現在の状態に依存する。

【0035】

CAでは、同じルールがすべてのセルに適用される場合、CAは均質なCAと呼ばれる。そうでなければ、それはハイブリッドCAと呼ばれる。様々な境界条件がある場合がある。すなわち、ヌル（端部のセルが論理「0」に接続される場合）、周期的（端部のセルが隣接する）、などである。

【0036】

CAの背景技術は非特許文献2で見つけることができる。

【0037】

2×Lセルオートマトン (2-by-L Cellular Automata) :

2×L CAは非特許文献4で提案され考慮されたが、このセクションでは2×L CAのある特性について簡単に説明する。

【0038】

上述したように、線形の有限状態機械 (LF SM) は、 L 個のシングルビット・メモリエレメントおよび1つの遷移関数で構成される。時間 t で i 番目のメモリエレメントの値または状態は、 s_i^t で示される。時間 t の LF SM の状態は、 s^t で示される。遷移関数 f は、時間 t の状態から時間 $t+1$ での LF SM の状態を決定する。すなわち $s^{t+1} = f(s^t)$ である。LF SM の次の状態関数は、グラフ式に状態図を使用して記述することができる。なお、LF SM の直線性は、 f が n ビット・ベクトルから n ビット・ベクトルまで線形関数であることを意味する。すなわち、任意の2つの状態 a および b について

$$f(a+b) = f(a) + f(b)$$

である。遷移関数 f は、 n 個の関数 f_1, f_2, \dots, f_n として特定することができる。ここで、 i 番目の関数がセル i の次の状態を計算する。

【0039】

$$s_i^{t+1} = f_i(s^t)$$

CAとの関連では、関数 f_i は、セル i についてのセルルールと呼ばれる。 f_i の各々が線形の場合、しかもその場合のみ、遷移関数 f は線形である。簡単のために、 s が現在の状態を示すために使用され、次の状態には s^+ が使用されるものとする。同様に、 s_i は現在の状態を示し、 s_i^+ はセル i の次の状態を示すものとする。CAにおいて、「セル間の通信が最近傍で行われる」とは、各セルがその直近の近傍だけに接続されることを意味している。図1は、2×1 CAの相互接続構造を示す。左端および右端のセルは、それらの左右の入力部（図では省略されている）で定数0入力をそれぞれ有すると仮定する。そのようなCAは、規則的な配置を有する2×1 CAと呼ばれる。

【0040】

各時間ステップにおいて、各セルは、そのセルルールを使用して、新しい状態を計算する。異なるセルは異なるルールを使用することができ、CAをハイブリッドとして構成する。さらに、CAが完全に接続されている、すなわち各セルがその近傍の内3つすべてから入力を受け取ると仮定すると、結果として、セル i についてのセルルール f_i は、下記のうちの1つであることになる：

【0041】

【数5】

$$f_i(s_l, s_r, s_v, s_s) = s_l \oplus s_r \oplus s_v \quad \begin{array}{l} \text{(セルがルール0} \\ \text{を用いた場合)} \end{array} \quad \dots(5)$$

【0042】

【数6】

$$f_i(s_l, s_r, s_v, s_s) = s_l \oplus s_r \oplus s_v \oplus s_s \quad \begin{array}{l} \text{(セルがルール1} \\ \text{を用いた場合)} \end{array} \quad \dots(6)$$

【0043】

ここで、 s_l (s_r) は、左 (右) 近傍の現在の状態を示し、 s_v は、縦方向の近傍のそれを示し、 s_s は、セル i 自体の状態を示す。ルール 0 およびルール 1 は、それぞれルール 90 およびルール 150 をそのまま一般化したもので、背景技術の一次元 CA 文献に開示されている。

【0044】

2つのルールだけしかいないため、セルによって使用されるルールは、シングルビットとしてコード化することができる、つまり、「1」はルール 1 を示し、「0」はルール 0 を示す。変数 t_1, t_2, \dots, t_L および b_1, b_2, \dots, b_L は、セルによって使用されるルールを示すために用いる。簡単のために、 t_1, t_2, \dots, t_L に対応して、トップセルは、1 から L まで番号が付けられ、 b_1, b_2, \dots, b_n に対応して、ボトムセルは、 $L+1$ から $2L$ まで番号が付けられる。一般に、ルール・ベクトル $[t_1, t_2, \dots, t_n], [b_1, b_2, \dots, b_n]$ は、与えられた 2×1 CA を識別するために使用される。

【0045】

LF SM の遷移行列 T は、遷移関数を代数的に定義するので、 $s^+ = s \cdot T$ である。一次元 CA の遷移関数は、三重対角 (tridiagonal) である。 2×1 CA について、遷移行列は、ブロック構造を持っている。

【0046】

【数7】

$$T = \begin{bmatrix} T_1 & I \\ I & T_2 \end{bmatrix} \quad \dots(7)$$

【0047】

ここで、 T_1 と T_2 が $L \times L$ の三重対角行列であり、 I は $L \times L$ 単位行列である。例えば、 2×4 CA についての遷移行列は以下のとおりである：

【0048】

【数8】

$$T = \left[\begin{array}{cccc|cccc} t_1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & t_2 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & t_3 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & t_4 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & b_1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & b_2 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & b_3 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & b_4 \end{array} \right] \quad \dots(8)$$

【0049】

ここで、 t_i および b_i ($1 \leq i \leq 4$) は上記のように定義される。なお、任意の 2×1 CA の遷移行列は対称である。

【0050】

2×3 CA の例を考慮し、CA がルール・ベクトル $[1, 1, 0], [0, 0, 1]$ を使用すると仮定すると、その結果は、以下のとおりである。

【0051】

$[t_1, t_2, t_3] = [1, 1, 0]$ 及び $[b_1, b_2, b_3] = [0, 0, 1]$
]

s_i ($1 \leq i \leq 6$) を現在とすると

【0052】

【数9】

$$s_1^+ = s_1 \oplus s_2 \oplus s_4$$

$$s_2^+ = s_1 \oplus s_2 \oplus s_3 \oplus s_5$$

$$s_3^+ = s_2 \oplus s_6$$

$$s_4^+ = s_1 \oplus s_5$$

$$s_5^+ = s_2 \oplus s_4 \oplus s_6$$

$$s_6^+ = s_3 \oplus s_5 \oplus s_6$$

【0053】

最小コストの $2 \times L - CA$ (Minimal Cost 2-by-L CA) :

任意のアプリケーションについて、一般に、LF SMインプリメンテーションのハードウェアコストを最小限にすることを試みるのが望ましい。1D CAに関し同様の方法で、500までの程度で最小コストの 2×1 CAが計算されたが、これは、非特許文献4で報告されている。なお、ハードウェアコストを最小限にすることは、ルール1を用いるセル数を最小限にすることを意味する。というのは、ルール1は、評価およびインプリメンテーションについて、わずかに高い複雑度を有するからである。

【0054】

与えられた 2×1 CAが最大長サイクルを持っているかどうか決めるために、非特許文献4で提案されたアルゴリズムは、以下のとおりである：

1. 非特許文献4に記述された定理1での回帰関係を使用して、CAの固有多項式を計算する、
2. 固有多項式がプリミティブかどうかをチェックし、もしそうであれば、CAは最大長サイクルを有する。

【0055】

従って、各 n ($1 \leq n \leq 250$) について、アルゴリズムは、最初に均質なルール0 CAを生成しチェックする。これが成功しない場合（その筈はないが）、アルゴリズムは、単一のルール1セルを備えた $2 \times n$ CAをすべて生成する。これが成功しない場合、アルゴリズムは、1対のルール1セルを有するCAをすべて生成する。そしてこれを続けていく。各 n について、検索は、最大長サイクルを有する最初の $2 \times n$ CAで止められた。従って、生成されたCAは、最小コストを有する、つまり、最も少ない数のルール1セルを使用する。アルゴリズムの結果は、非特許文献4の表3に示されている。

【0056】

なお、 $L=2$ および $L=4$ については、最大長サイクルの $2 \times n$ CAが存在しない。 2×2 CAの構造は、周期的な線形のハイブリッドCAと同じである。したがって、最大長マシンがないのは驚くことではない。

【0057】

非特許文献4中で計算した結果は、均質な重み1 CAに関する2つの観察につながる。セルがすべて同じルールを使用する場合、CAは均質である。そのようなCAは、セルがすべてルール0を用いる場合ルール0 CAと呼ばれ、あるいは、セルがすべてルール1を使用する場合、ルール1 CAと呼ばれる。重み1 CAは、ルール1を用いる単一のセルとルール0を使用する全ての残りのセルとを有する。非特許文献4の中で報告された観察は次のとおりである：

- ・観察1. 最大長の均質CAは、存在しない。
- ・観察2. $L > 1$ の場合、最大長の重み1 CAは存在しない。

【0058】

本実施形態による装置および方法：

初めに、制御可能な周期を有する擬似乱数シーケンスを生成する第1の実施形態による方法を説明する。

【0059】

バイナリのシーケンス $\{a_i\}_i$ および $\{b_i\}_i$ は、2つの独立プロセスの実現であり、下記が有効であると仮定する。

- ・シーケンス $\{a_i\}_i$ を生成するプロセスは、実験によって評価された少なくとも適度な周期と、統計的テストのシステムで測定された望ましいランダム性特性を有するシーケンスを提供する。

- ・シーケンス $\{b_i\}_i$ を生成するプロセスは、値が分析的に証明可能である長い周期と、統計的テストのシステムで測定された少なくとも適度なランダム性特性を有するシーケンスを提供する。

【0060】

そして、本出願の発明者は以下が有効であること発見した。

- ・シーケンス $\{c_i\}_i = \{a_i \text{ 「○+」 } b_i\}_i$ は、値が分析的に証明可能である長い周期と、統計的テストのシステムによって測定された望ましいランダム特性とを有する。

【0061】

上記の知見によれば、高いランダム性特性および制御可能な周期を有する、バイナリのシーケンスを生成する下記方法が提供され、該方法は以下のステップを含む：

- (1) 適切なセルオートマトンに基づいたアプローチを使用して、所望のランダム特性および予期された周期の（少なくとも）適度な長さを備えたバイナリのシーケンスを生成するアルゴリズムを特定する；

- (2) 適切なセルオートマトンに基づいたアプローチを使用して、所望の周期および（少なくとも）適度なランダム特性のバイナリのシーケンスを生成するアルゴリズムを特定する；

- (3) 上記2つの要素シーケンスのビット毎 $\text{mod } 2$ の和として、結果として生じるシーケンスを生成する；結果的に生じるシーケンスについて予期される特性は、所望の統計特性およびシーケンス周期の制御可能な下限である。

【0062】

次に、制御可能な周期を有する擬似乱数シーケンスを生成する第1の実施形態による装置の一例について説明する。制御可能な周期の擬似乱数シーケンスを生成する装置のための3つの主要な構成要素は次のとおりである：

- ・図1に表示され、上記セクションおよび表1で特定される $2 \times L \text{ CA}$ ；
- ・図2に表示され、表2（詳細に関しては上記セクションを参照）に基づいて特定される $2D \text{ CA}$ ；および
- ・ $2 \times L \text{ CA}$ および $2D \text{ CA}$ から生じるシーケンスのビット毎 $\text{mod } 2$ の和のための加算器。

【0063】

【表 1】

L	2×L CA 仕様
3	1, 2, 6
32	8, 13
64	1, 4, 46
96	5, 10
128	2, 226

【0064】

【表 2】

ルール15	$s_{i,j}(t+1) = s_{i-1,j}(t) \oplus s_{i,j-1}(t) \oplus s_{i+1,j}(t) \oplus s_{i,j+1}(t)$
ルール31	$s_{i,j}(t+1) = s_{i-1,j}(t) \oplus s_{i,j-1}(t) \oplus s_{i+1,j}(t) \oplus s_{i,j+1}(t) \oplus s_{i,j}(t)$
ルール47	$s_{i,j}(t+1) = 1 \oplus s_{i-1,j}(t) \oplus s_{i,j-1}(t) \oplus s_{i+1,j}(t) \oplus s_{i,j+1}(t)$
ルール63	$s_{i,j}(t+1) = 1 \oplus s_{i-1,j}(t) \oplus s_{i,j-1}(t) \oplus s_{i+1,j}(t) \oplus s_{i,j+1}(t) \oplus s_{i,j}(t)$

【0065】

表1は、複数個の特定の2×L CAを特定する。表中のエントリは、どのセルがルール1を使用するか示す。例えばエントリ

3 1, 2, 6

は、2×3 CAのルールベクトルを表す。つまり、6つのセルのCAについてのルールベクトルは

以下の通りとなる。

【0066】

$[[t_1, t_2, t_3], [b_1, b_2, b_3]] = [[1, 1, 0], [0, 0, 1]]$

ここで、「1」は、セル1、2および6のルール1を示す。

【0067】

本装置は、高品質の疑似乱数シーケンスを生成する、非特許文献1で報告されている特定の2D-CAを使用する。これは、二次元(2D)の8×8の配列に整えられた64のセルからなる。

【0068】

$s_{i,j}(t)$ は、時刻 t 、 $i, j = 1, 2, \dots, 8$ に、座標 (i, j) を有する2D-CAのセル状態を示すとする。使用される2D-CAでは、セルは、表2で与えられるルールのうちの1つに従って更新される。使用される2D-CAは、図2に示す。

【0069】

図3は、本発明の第1の実施形態による装置の配置例を示す。本装置は、2D-CA 310、2×L CA 320、2D-CAセル出力および対応する2×L CAセル出力のビット毎mod 2加算を行なう加算器330-1, 330-2, ..., 330-n、および生成された高品質の制御可能な周期の疑似乱数シーケンス350を出力するために、mod 2加算演算結果をバッファするバッファ340を有する。ここで、高品質疑似乱数シーケンスとは、シーケンス・ランダム性を測定する指定された統計的なテスト群をパスするシーケンスを意味する。

【0070】

本装置は、CPUとメモリを備えたコンピュータに所定のプログラムを実行させたり、あるいは、ハードウェアロジック装置により実現することができる。

【0071】

図3に示された本装置は、以下のように動作する。

- ・初期化：独立したランダム・ビットのシーケンスを用いて、すべてのセルを初期化する。
- ・シーケンス生成：本装置の各サイクルは、次のステップからなる：
 - (1) $2 \times L$ C A 3 2 0 を1サイクル動作させ、その全てのセルを更新する；
 - (2) $2 D - C A 3 1 0$ を1サイクル動作させ、その全てのセルを更新する；
 - (3) $2 D - C A 3 1 0$ のセルと対応する $2 \times L$ C A 3 2 0 のセルとのビット毎mod 2加算を行なう。

【0072】

次の表3は、本装置の空間複雑度および出力シーケンス周期の得られた下限の典型的な値を示す。

【0073】

【表3】

使用された C Aセル数	出力シーケンス 周期の下限
128	2^{64}
160	2^{96}
160	2^{96}

【0074】

第2の実施形態：

本発明の第2の実施形態によれば、ストリーム暗号(stream cipher)を設計するための構築ブロックのファミリーが提供される。これらの構築ブロックの主な役割は、後段処理に好適な擬似乱数シーケンスを生成することである。これらのシーケンスは、高度なランダム性特性、長い周期を有しており、実用上予測不可能なものである。本実施形態の構築ブロックは、出力擬似乱数シーケンスの所望特性を実現するように組み合わせられた3つの異なるクラスのセルオートマトンに基づいている。本実施形態のファミリーは、広い範囲における特定のインプリメンテーションまたはアプリケーション制約に好適な、あるファミリーメンバを選択できるという可能性を与えている。

【0075】

ストリーム暗号用の適切な基礎的構築ブロックの開発は、良く認識されており、開かれた課題である。極めて最近、非特許文献5で、このトピックへの新たな寄与が報告されており、T関数に基づいた暗号構築ブロックが研究されている。

【0076】

しかしながら、その課題に取り組むために異なるアプローチを提供することによって、ユーザーあるいはシステム設計者に、擬似乱数シーケンスを生成する、より柔軟な手段を提供することが望ましい。例えば、セルオートマトンの利用に基づいたストリーム暗号について、適切な構築ブロックを得るために新たなフレームワークを提供することが望ましい。本実施形態について詳細に説明する前に、本実施形態中で使用されるC C Aの基礎技術のうちのいくつかについて説明する。

【0077】

制御可能なセルオートマトン(C C A:Controllable Cellular Automata)：

本セクションでは、非特許文献6で紹介された、制御可能なセルオートマトン(C C A)の概要を述べる。詳細な説明は非特許文献6に開示されている。C C Aの説明に当たり、C C Aの特性を識別するためにいくつかの点について最初に定義する。

- ・定義：C C Aは、いくつかのセルの動作(どのようにセルの状態が各サイクルで更新さ

れるか)が、セル制御信号によって制御することができるCAである。ルール制御信号と同様に、セル制御信号はROMに格納するか、あるいはCAによって生成することができる。

・定義：セルが、セル制御信号で制御される場合、それは制御可能なセルである；そうでなければ、それは基本セルである。CCAは、制御可能なセルおよび基本セルの組み合わせである。制御可能なセルおよび基本セルの双方は、ルール制御信号を有し得る。

【0078】

制御可能なセルの動作は、その現在のセル制御信号によって決定される。制御可能なセルは、ノーマルとするか(セル制御信号が0である場合)、あるいはアクティブ(セル制御信号が1である場合)にすることができる。制御可能なセルがノーマルな場合、制御可能なセルおよびその近傍の状態の計算は、(現在のルール制御信号およびその近傍の状態によって)通常とおりである。制御可能なセルがアクティブな場合、制御可能なセルおよびその近傍の状態の計算は、いくつかの予め定められた動作によって特定される。制御可能なセルおよびその近傍に適用された動作は相違し得る。予め定められた動作が制御可能なセルの状態計算に影響することになる。

【0079】

CCAの構造は、合計でL個のセルを有する。M($M \leq L$)セルは、制御可能なセルであり、残りのセルは基本セルである。ここで、基本セルは、すべてプログラム可能なセルである。したがって、このCCAでは、ルール制御ビットおよびセル制御ビットがある。ルール制御ビットを有する、Lセルのプログラム可能なCA(PCA)と比較して、CCAの追加コストは、Mセル制御ビットである。CA遷移中に、どのルールを、基本および制御可能なセルの双方上で使用すべきか、ルール制御信号が決定し、セル制御信号は、制御可能なセルの状態を決定する。

【0080】

CCAの制御可能なセルの使用により、それとプログラム可能なCA(PCA)(ルール制御信号だけが存在する)を区別する。一旦制御可能なセルおよび基本セルの動作が特定されれば、制御可能なセルのセッティングは、CCAの性能を決定する。PCAとCCAでの共通の概念は、CA遷移を、より予測不能でより柔軟にするために、CAセルについて、それらが双方とも、いくつかの制御ラインを使用するということである。相違点は、PCAでは全てのセルが均質な構造を有し、一方、明らかにCCA中では、制御可能なセルの構造は基本セルのそれと同じではないということである。

【0081】

同様のCAの性能を達成するために、他の方法を使用してもよい。例えば、半径(つまり近傍の数)を増加させたり、各セル中でより多くの状態を使用したり、または各セルのルール・テーブルを発展させたりすることである。コストが比較可能ではないので、どの方法が、性能またはハードウェア設計において良いのか言うのは難しい。ルール・テーブルを発展させる代わりに、セル状態を変える場合、異なる計算アプローチを適用することができるように、CAセルの状態を制御するスキームが提案されている。これに基づいて、進行中にセル状態を変更することができるCA-CCAの新しいクラスは、非特許文献6で提案されている。その研究は、当時良好なランダム性品質を得ることができるCCAの良い構成を見つけることに焦点を絞っていた。

【0082】

下記では、2つの制御可能なセルタイプが提案されており、これらは、性能をさらに検討するためにCCAの例として用いられる。

【0083】

上述のように、セル制御信号が0である場合、制御可能なセルは基本セルと同じ動作をとる。一方、セル制御信号が1である場合、制御可能なセルは予め定められた動作を実行する。つまり、ノーマルな場合にそれが行なう動作とは相違し得る。これは、アクティブな場合、制御可能なセルが行なう動作が、制御可能なセルの特性を決定することを意味する。

【0084】

アクティブにされた制御可能なセルが実行できる最も単純な動作は、CA計算プロセスの間に、その状態を維持することである。その間に、通常通り、その近傍の状態が計算される。この種の制御可能なセルは、タイプ0の制御可能なセルと呼ばれる。タイプ0の制御可能なセルおよび基本セルの組み合わせであるCCAは、以下ではCCA0と呼ぶ。

【0085】

制御可能なセルがアクティブとされた場合、タイプ2の制御可能なセルとなり、その最新の状態を維持するが、その近傍はそれをバイパスする。つまり、これは、アクティブにされた制御可能なセルが、その近傍の状態計算に関係しないということである。このように、近傍関係は、CA計算プロセスの間に、ダイナミックに変更される。タイプ2の制御可能なセルと基本セルとの組み合わせであるCCAは、CCA2または近傍変更CA(NCA)と呼ばれる。その近傍変更挙動のためにCCA2は、どんなPCAによってもシミュレートすることができない。

【0086】

本実施形態による装置および方法：

例えばストリーム暗号のための、本実施形態による新たな構築ブロック・ファミリのデザインに対する基本的な構想には、下記が含まれている。

(1) 最近報告されたセルオートマトンと、構築ブロック出力シーケンスの次の2つの特性を制御するための背景技術を与えるCAベースの疑似乱数生成器との使用：

- ・統計特性(ランダム性)、
- ・周期、

(2) 時間変化アルゴリズムを生成に利用することによって、構築ブロック出力シーケンスの非予期性を提供すること、特に下記を提供すること：

- ・報告された改善された速い相関性攻撃(例えば、非特許文献8参照)および代数的攻撃(例えば、非特許文献9参照)に対する耐性。

【0087】

構築ブロックは複数の部から構成され、その各々は、次の項目、つまり、長い周期、良好な統計、非予期性のうちの1つまたは2つに寄与する。

【0088】

本実施形態の設計では、セルオートマトンは主要素として使用される。CAと関連する次の最近の報告が考慮されている。

・非特許文献1および6は、CA構造を指摘しているが、これらは、非特許文献11で示した表4中で列挙された多数の統計的テストをパスすることができる高いランダム性のバイナリシーケンスを生成する2D-CA(2次元セルオートマトン)およびCCA(制御可能なセルオートマトン)である。表4はダイハート(DIEHARD)テスト集として知られている。

・非特許文献4中で報告されている結果は、分析上の立証可能性(上記セクションも参照)を有する、最大の周期シーケンスを生成するCA構造を指摘している。

【0089】

【表 4】

インデックス 番号	テスト名	グレード
1	Overlapping Sum	P 値が 0 又は 1 ではない場合、 合格と見なす。
2	Runs up 1	
	Runs Down 1	
	Runs up 2	
	Runs Down 2	
3	3D Sphere	
4	A Parking Lot	
5	Birthday Spacing	
6	Count the Ones 1	
7	Binary Rank 6*8	
8	Binary Rank 31*31	
9	Binary Rank 32*32	
10	Count the Ones 2	
11	Bitstream Test	
12	Craps Wins	
	Craps Throws	
13	Minimum Distance	
14	Overlapping Permutation	
15	Squeeze	
16	OPSO Test	
17	OQSO Test	
18	DNA Test	
18	Overall KS Test	

【0090】

本実施形態では、次の3つの主要素を構築ブロックに使用することができる：

- ・図1に表示された、表1中で挙げられた特定の例を有する第1の実施形態の説明において指定された2×L CA
- ・図2に表示され、表2に基づいた第1の実施形態の説明で指定された2D-CA；
- ・図4～5に表示され、表5中で特定されたCCA；および
- ・2×L CA、2D-CAおよびCCAから結果的に生じるシーケンスのビット毎mod 2の合計のための加算器。

【0091】

【表 5】

セル インデックス 間隔	1-10	11-20	21-30	31-40	41-50	51-60	61-64
セル更新 ルール	0110101111	0010110001	1100101011	1101111011	1100110001	0001000000	1111
セル計算 ルール	0000111110	0000011010	1111100010	0101100111	1001010111	1000110111	1101

【0092】

使用されたC C A構造は表5で特定されるが、これは、最適化（進化した多目的最適化：evolutionary multi objective optimization: E E O O）アルゴリズムによって得られ、最良の統計特性を有するものの一つとして非特許文献6で報告されている。表5の第2行では、「1」は制御可能なセルを示し、また、第3行では、「1」はC C A出力に寄与するセルを示す。

【0093】

図4は、本実施形態の装置でC C Aを含む全体的なブロック構造の例を示す。図5（B）は、C C Aの内部構造の一例を示す。また、図5（A）はC C Aを構成するセルユニットの構造の一例を示す。

【0094】

図4で示すように、本実施形態では、C C A 4 0 0についてのルール制御信号（ルール制御ワード）およびセル制御信号（セル制御ワード）が、2つのC A 4 0 1, 4 0 2によって別々に生成されると仮定する。ルール制御信号を生成するC A 4 0 1は、ルール制御C Aと呼ばれる。セル制御信号を生成するC A 4 0 2は、セル制御C Aと呼ばれる。

【0095】

図5（B）で示すように、C C A 4 0 0は、複数個のセルユニット5 1 0-1, . . . , 5 1 0-i, . . . , 5 1 0-j, . . . , および5 1 0-Lを含んでいる。本例においては、C C A 4 0 0が、合計でL個のセルを有しており、M ($M \leq L$) 個のセルが制御可能なセル（例えば、セルユニット5 1 0-i, 5 1 0-j）であり、残りのセルが基本セル（例えば5 1 0-1, 5 1 0-L）であると仮定している。制御可能なC Aセルユニットは、例えば図5（A）で示すように、セル5 1 0 1（その状態は、セル制御信号およびルール制御信号によって制御される）と、左右近傍セルの状態を入力するための加算器5 1 0 2とを有している。

【0096】

ここで、基本セルは、すべてプログラム可能なセルである。したがって、このC C Aには、ルール制御ビットおよびセル制御ビットがある。ルール制御ビットを有する、Lセルのプログラム可能なC A（P C A）と比較して、C C Aの追加コストはMセル制御ビットである。C A遷移中に、制御信号は、どのルールを基本および制御可能なセル上で使用するか決定する。セル制御信号は、制御可能なセルの状態を決定する。

【0097】

各サイクルで、C C Aセルについてのルール（セル）制御信号のビット組み合わせは、ルール（セル）制御ワードと称される。ルール制御ワードの長さは、C C A 4 0 0のそれと同じであり、一方、セル制御ワードの長さは、C C A 4 0 0中の制御可能なセルの数によって決定される。

【0098】

C C A 4 0 0のランニングシーケンスは、次のように説明される。初期シードおよび遷移ルールは、それらを初期化するために、ルール制御C A 4 0 0、セル制御C A 4 0 2およびC C A 4 0 0へ入力される。C C Aセルについて、ルールおよびセル制御ワードを生成するために、2つの制御C A 4 0 1, 4 0 2が、C C A 4 0 0と同期して作動する。各サイクルにおいて、C C Aセルの前の状態およびルール／セル制御ワードは、C C Aセルの現在の状態を決定する。いくつかのC C Aセルの現在の状態は、出力ビットシーケンスとして、すべてのサイクルで記録される。

【0099】

非常に多くの研究がP C Aでの良好な遷移ルールの探索のために行われているため、非特許文献6では、勧められたルールを選択している。非特許文献6で使用される4つの加法ルールは、ルール9 0、1 5 0、1 0 5および3 0である。ルール9 0および1 5 0は、C C A中で遷移ルールとして使用される。これは、1ビットP C A 9 0 1 5 0との比較を容易にする。ルール3 0はルール制御C A中で使用され、ルール1 0 5はセル制御C A中で使用されるが、これら2つのルールが、非特許文献7によると、乱数発生で最良のものと言われているからである。なお、64のセルを備えた非特許文献6で記述・使用され

たCCA(CCA2)においては、35の制御可能なセルおよび35の出力セルがあり、20は制御可能なセルである。

【0100】

本発明の本実施形態によれば、上述の構築ブロック(3-CA)のファミリーを含む装置が提供される。本装置は、制御可能な周期を有する、実用上予測不能な高品質の疑似乱数シーケンスを生成する。

【0101】

典型的な3-CA構築ブロックを備えた装置を、図6に示す。本装置は、2D-CA310と、2×L CA320と、CCA400と、2D-CA310、2×L CA320およびCCA400からの対応するセル出力のビット毎mod2加算を行なう加算器600-1、600-2、...、600-nと、生成した高品質疑似乱数シーケンス650を出力するために、mod2加算演算結果をバッファするためのバッファ340と、を有する。

【0102】

さらに、本実施形態の装置では、2D-CA310および2×L CA320は、ルール制御CA401およびセル制御CA402としてそれぞれ機能する。言い換えれば、ルール制御ワード610およびセル制御ワード620は、2D-CA310および2×L CA320からそれぞれ生成され、図4および図5で示されるようにセルおよびルール制御用のCCA400に供給される。

【0103】

図6に示された本装置は、以下のように動作する。

- ・初期化：独立したランダム・ビットのシーケンスを用いて、すべてのセルを初期化する。
- ・シーケンス生成：3-CA構造の装置の各サイクルは、次のステップを含む：
 - (1) 2×L CA320を1サイクル動作させ、その全てのセルを更新する；
 - (2) 2D-CA310を1サイクル動作させ、その全てのセルを更新する；
 - (3) 2D-CAセルに基づいたCCARルール制御ワードを特定する；
 - (4) 2×L CAセルに基づいたセル制御ワードを特定する；
 - (5) CCAを1サイクル動作させ、その全てのセルを更新する；および
 - (6) 対応するCCA、2D-CAおよび2×L CAセルのビット毎mod2加算を行なう。

【0104】

表6は、使用されたCAセルの総数および出力シーケンス周期の得られた下限によって測定された構築ブロック空間複雑度の例を示す。

【0105】

【表6】

使用されたCAセル数	出力シーケンス周期の下限
128	2^{64}
256	2^{128}

【0106】

第3の実施形態：

本発明の第3の実施形態では、暗号の疑似乱数シーケンス生成器(キーストリーム生成器)のファミリーは、ストリーム暗号の設計および関連するアプリケーションのために提供される。本実施形態のファミリーは、高効率とセキュリティを同時に生む。本実施形態のキーストリーム生成器は、高いランダム特性、長い周期のシーケンスを生むものであり、実

用上予測不能である。

【0107】

本実施形態のキーストリーム生成器は、出力疑似乱数シーケンスが所望特性を生むように組み合わせられた、3つの異なるクラスのセルオートマトン、ラテン方格に基づいた非線形マッピングおよび不均一な間引き処理に基づくものである。

【0108】

ストリーム暗号用の適切な暗号疑似乱数シーケンス生成器またはキーストリーム生成器の開発は、良く認識されており、開かれた課題である。多くの根本的な要素およびキーストリーム生成器は、関連する技術文献の中で報告されている。報告されたスキームのうちのいくつかは、セルオートマトン(CA)に基づく。

【0109】

元々、セルオートマトン(CA)は、自己複製の構造を調査するために1950年代の初めにフォン・ノイマンによって提案された。CAに基づく疑似乱数発生器(PRNGs)についての関心の増大は、その単純さおよびカスケード構造のためであり得る。CAは、規則的であり、ローカルに相互連結することができ、そしてモジュール式である。これらの特性のため、ハードウェア中でCAをインプリメントすることが、他のモデルよりも簡単になる。CAは、乱数シーケンスを、連続あるいはパラレルのいずれかで生成することができる。實際上、ほとんどのCAでは、より高い作業効率を得るために、シーケンスをパラレルに生成する。

【0110】

セルオートマトンはセルのアレイであり、各セルは、許容可能な状態のうちの任意の1つをとることができる。各離散時間ステップ(時計サイクル)では、セル状態の変更は、その遷移ルールに依存し、これはk近傍CAについて、そのk近傍の現在の状態の関数である。セルアレイ(グリッド)は、n次元であるが、ここで、 $n=1, 2, 3$ が実際に使用される。XORおよびXNORルールの組み合わせがあるCAは、加法的(additive)CA(非特許文献3)と呼ばれる。CAセルがすべて同じルールに従う場合、CAは均質で(uniform)あると言う；そうでない場合、それは不均一(non-uniform)か、あるいはハイブリッド(非特許文献7)である。CAは、端部のセル(最初のセルおよび最後のセル)が互いに隣接している場合に、周期的境界CA(PBCA)であると言う。CAは、端部のセルが、その左(右)セル(非特許文献3)のみに接続される場合に、ヌル境界CAであると言う。

【0111】

加法的セルオートマトン(Additive Cellular Automata)：

CAの非常に重要なクラスは、GF(2)における線形CAまたは加法的CAである。次の状態を生成する論理が、XORまたはXNOR演算だけを使用する場合、CAは加法的CAであると言う。線形のCAは、線形の有限状態機械(LFSM)の特定な形である。すべてのLFSMは、GF(2)の上の遷移行列によって一義的に(uniquely)表わされ、すべての遷移行列は、固有多項式を有する。

【0112】

XOR演算だけを備えたLセルの一次元加法的CAについては、Tで示された線形演算子が、CAを特徴づけ得ることが、非特許文献12の中で示されているが、Tは、 $L \times L$ ブール行列であり、そのi番目の行は、i番目のセルの近傍依存性を特定する。CAの次の状態は、列ベクトルとして表わされる現在のCA状態のこの一次演算子を適用することにより生成される。演算は、正規行列乗算であるが、含まれている加算は、モジュール2合計である。 $x(t)$ が、t番目の時刻のオートマトンの状態を表わす列ベクトルであれば、オートマトンの次の状態が、以下で与えられる：

$$x(t+1) = T \times x(t)$$

CAの固有多項式がブリティブな場合、それは最大長CAと呼ばれる。そのようなL個のセルからなるCAは、全0状態を除き、連続サイクルで $2^L - 1$ の状態すべてを生成する。

【0113】

固定次数 L については、 $2^L \times 2^L$ 遷移行列（従って、 $2^L \times 2^L$ の LFSM）があるが、 2^L 次の L 多項式だけであるので、次の状況がある： L セル LFSM と $L \times L$ 行列の間に一対一対応があり、そして同時に、遷移行列と L 次の多項式の間に多対一の対応がある。

【0114】

LFSM の固有多項式を得ることは難しくない。というのは、行列式の評価によりそれを計算することができるからである。他方では、特定の固有多項式で特定のタイプの LFSM（CA のような）を見つけることは、非特許文献 13 の中で解決された課題である。ここでは、与えられた固有多項式を有する CA を得るための方法が示されている。当該方法は、各既約多項式について、CA が存在するか否かの課題を解決するためにも使用することができる。

【0115】

プログラム可能なセルオートマトン（Programmable Cellular Automata）：

ルール 90 およびルール 150 の位置表現は、近傍依存性が単に 1 つの位置において、すなわちセル自体上で異なることを示している。したがって、1 つのセルについて単一の制御線を配することによって、異なる時間ステップに、ルール 90 およびルール 150 の双方を同じセルに適用することができる。そのために、 L 個のセル CA 構造は、 2^L 個の CA 配置を実現するために使用することができる。同じ構造上で異なる CA 配置（ルールを更新するセル）を実現することは、適切なスイッチを制御するために、制御論理を使用して達成し得る。また、ROM に格納された制御プログラムは、制御をアクティブにするために使用することができる。ROM ワードの i 番目のビットの 1 (0) 状態は、 i 番目のセルを制御するスイッチを閉じる（開く）。このような構造は、プログラム可能なセルオートマトン（PCA）と呼ばれる。

【0116】

従って、更新するルールを形成するセル当たり 1 つの操作量を配して、そのセル（ルール 90 あるいはルール 150 の）に適用することができる。ルール 90 (150) が、 i 番目のセルに適用される場合、 n セル PCA のための n ビット制御ワードは、 i 番目のセルの上に 0 (1) を有する。

【0117】

セルオートマトンに基づく疑似乱数生成器：

本実施形態が適用される CA の疑似乱数生成器（PRNG）は、研究が盛んな分野であった。非特許文献 3 は、最大長の CA によって生成されたパターンのランダム性が、線形のフィードバック・シフトレジスタ（LFSR）のような他に広く用いられている方法よりも著しくよかったことを示している。

【0118】

複数の論文では、ある PCA と同様に一次元の $(1-d)$ CA PRNG も議論された。しかしながら、これらが、まだいくつかのランダム性テストを通らないので、 $1-d$ PCA でも、ランダム性品質は、完全には満足できるものではない。

【0119】

CA のランダム性を改善するために、いくつかのセルに、セル制御信号を加えることにより、 $1-d$ PCA を増強し、かつ CA の状態を制御するアプローチが報告されている（非特許文献 6 を参照）。最初の概念は、さらに洗練されて、近傍変更 CA（NCA）の概念になった。 $1-d$ NCA に関するランダム性テスト結果は、それらが $1-d$ PCA よりも良いことを示した。非特許文献 6 では、 $1-d$ NCA は、最小のコストを備えた最良のパフォーマンスまで進展した。

【0120】

他方、代案として、CA PRNGs のランダム性品質をさらに改善するために、疑似乱数生成に二次元の $(2-d)$ CA を使用するアプローチが報告された。非特許文献 1 では、非特許文献 11 のダイハードテストをパスし得る 64 セルの $2-d$ CA を進展させたことが報告されており、これは、現在では、パスするのが最も困難なテスト群であると

言われている。ランダム性テスト結果の比較は、2-d CAがランダム性において、1-d NCAに匹敵する。しかし、2-d CAの構造の複雑度は、1-d CAと比較して多少高い。

【0121】

近年、GF(2)の上の線形セルオートマトンに基づいた2つのキーストリーム生成器(ROMおよび2ステージPCAを備えたPCAと呼ばれる)が、それらの安全性分析(security analysis)の結果と共に、非特許文献14中で提案された。

【0122】

他方、中央のCAセルによって生成されたビットのシーケンスに基づいたバイナリ(non-linear)のCA初期状態を再構築する方法が、非特許文献15中で与えられている。GF(2)上の非線形の置換ルールおよびCAを仮定して、所与の状態のプリデセッサ(predecessor)を計算する転位アルゴリズムが、非特許文献16中で提案されている。

【0123】

2ステージPCAおよびROMを備えたPCAの暗号の安全性分析は、非特許文献17および18の中でそれぞれ報告されており、ここで、ある暗号解読の攻撃のこれらのスキームのいくつかの脆弱性が、暗号文のみの攻撃(ciphertext only attack)と仮定して、実証されている。また、有効な秘密鍵サイズが、その正式の長さより著しく小さいことが示されている。同じ弱点は、既知の平文攻撃(plaintext attack)を仮定する非特許文献19中で指摘されている。

【0124】

近年、ROMを備えたPCAに基づく改善されたキーストリーム生成器が非特許文献20で、GF(2)上の演算を仮定して、提案され分析されている。GF(q)($q > 2$)上のCAのキーストリーム生成器アプリケーションが非特許文献10で報告されている。

【0125】

本実施形態による装置および方法:

本実施形態によるキーストリーム生成器は、 α ブロックおよび β ブロックと呼ばれる以下の2つの部分を備えている:

- ・第1の部分 α ブロックは次を提供する;
 - *長い周期
 - *良好な統計
 - *基本的な非予期性
- ・第2の部分 β ブロックは次を提供する;
 - *増強された最終非予期性。

【0126】

α ブロックの設計に対する根本的な概念は、次を含んでいる:

(1) 最近報告されたセルオートマトンと、構築ブロック出力シーケンスの次の2つの特性を制御するための背景技術を与えるCAベースの疑似乱数生成器との使用:

- ・統計特性(ランダム性)、
- ・周期、

(2) 時間変化アルゴリズムをその生成に利用することによって、 α ブロック出力シーケンスの非予期性を提供すること、特に下記を提供すること:

- ・報告された改善された速い相関性攻撃および代数的攻撃に対する耐性。

【0127】

α ブロックは、複数の部からなる構築ブロックを含むよう構成され、その各部は、次の項目のうちの1つあるいは2つに寄与する:

- 長い周期、
- 良好な統計、
- 非予期性。

【0128】

α ブロックの構造は、 $2 \times L$ CA、 $2D$ -CAおよびCCAを含んでいるが、これは

上述の実施形態に詳細に説明されている。同様の要素は、同じ番号によって指定されるので、その説明は簡単のために省略する。

【0129】

β ブロックの主な役割は、 α ブロックからの出力シーケンスの非予期性を増強することにある。

【0130】

α ブロックからの出力シーケンスが、バッファされ、 β ブロックによる処理が、次の2つの操作によって行なわれることが考えられる：

- ・メモリによる非線形関数によるフィルタリング、および
- ・前のステップから得られたシーケンスの不均一間引き (non-uniform decimation)。

【0131】

β ブロックで行なわれる処理の例は、図7と図8に示されている。図7は、非線形関数F1 (701) およびF2 (702) を使用して、メモリによる非線形マッピングのブロック構造例を示す。バッファ700は、 α ブロックからの出力シーケンスを記憶する。図8は、非線形関数F1 (701) およびF3 (703) を備えた、不均一間引きのブロック構造例を示す。間引手段800は、非線形関数F3からの出力の制御下で、非線形関数F1からの出力シーケンスを間引きする。

【0132】

図9は、使用された非線形マッピングの一般的な形態の例を示す。使用された関数F1、F2およびF3の各々は、ラテン方格 (LS) に基づいた一般的な非線形マッピング構造に従う。

【0133】

使用された非線形関数の各々は、図9で示されるような複数個のラテン方格テーブルからなる。これらのラテン方格テーブルの各々は、マッピング $\{0, 1\}^M \times \{0, 1\}^M \rightarrow \{0, 1\}^M$ を行なう。典型的なケースでは、各非線形関数は、2つのレイヤ (すなわち、レイヤ1、レイヤ2) からなる構造である。レイヤ1は、複数個のラテン方格テーブル $901-1, 901-2, \dots, 901-i$ からなり、レイヤ2は、複数個のラテン方格テーブル $901-j, \dots, 901-k$ からなる。

【0134】

図8で示される処理では、キーストリーム生成器は、非線形関数F3 (703) から出力された間引きワードの重みに応じて、生成されたビットを出力することなく完全なサイクルを複数回行なう。

【0135】

図10は、キーストリーム・シーケンス生成器のブロック構造例を示す。キーストリーム・シーケンス生成器は、次のものを備えている：

- 3つの異なるクラスのセルオートマトン310、320、400 (CA) ；
- ラテン方格に基づいた3つの異なる非線形関数701-703、つまりF1、F2およびF3、F1とF2はメモリを備えた非線形のコンバイナ／フィルタの役割をする；
- 基本的なキーストリーム・シーケンスの不均一間引きブロック800。

【0136】

本実施形態では、CAの3つの異なるクラスとして、 $2 \times L$ CA 320、2次元CA (2D CA) 310および制御可能／プログラム可能なCA (CCA) 400が使用される。各CAの詳細な特性は、第1および第2実施形態の説明における該当箇所に上述されている。なお、使用されたセルの総数は、本実施形態におけるファミリパラメータのうちの1つである。

【0137】

使用された3つのCAが、3-CAと呼ぶ下部構造を形成する。これらの3つのCAは、該3-CA下部構造が結果として下記を生むような方法で組み合わせられている：

- 高い非線形 (および非予期性) ；
- 出力シーケンスの周期の保証された下限 ；

ー出力シーケンスの検証された統計特性。

【0138】

図10に示された3-CA構造は、以下のように作動する：

- ・初期化：独立したランダム・ビットのシーケンスを用いて、すべてのセルを初期化する。
- ・シーケンス生成：3-CA構造の各サイクルは、次のステップを含む：
 - (1) $2 \times L$ CAを1サイクル動作させ、その全てのセルを更新する；
 - (2) $2D-CA$ を1サイクル動作させ、その全てのセルを更新する；
 - (3) $2D-CA$ セルに基づいたCCAルール制御ワードを特定する；
 - (4) $2 \times L$ CAセルに基づいた状態制御ワードを特定する；
 - (5) CCAを1サイクル動作させ、その全てのセルを更新する；および
 - (6) 対応するCCA、 $2D-CA$ および $2 \times L$ CAセルのビット毎mod 2加算を行なう。

【0139】

従って、キーストリーム生成器の動作は、初期化およびキーストリーム生成の2つのステップを含んでいる。

【0140】

キーストリーム生成器の初期化は、いずれのキーストリーム生成の前でも必要である。キーストリーム生成器の再同期は、初期化と同じ動作を仮定する。

【0141】

初期化の主なステップは、下記のとおりである：

- ーすべてのCAセルの初期値を設定すること；
- ーいかなる出力もなしに、キーストリーム生成器をM回動作させる、ここで、Mはキーストリーム生成器ファミリのパラメータである。

【0142】

次に、各動作サイクルでは、キーストリーム生成器内のキーストリーム生成の主な動作が実行される。キーストリーム生成には、次のものが含まれる：

- (1) すべてのCAの更新；
- (2) 非線形関数出力の生成；
- (3) 間引きルールに応じて、ステップ(4)に行くか、またはステップ(1)および(2)を繰り返す；および
- (4) 出力シーケンスブロック(キーストリームブロック)の生成。

【0143】

上述のように、本実施形態によるキーストリーム生成器は、広い範囲における特定のインプリメンテーションまたはアプリケーション制約に好適な、あるファミリメンバを選択できるという可能性を与えている。本実施形態のキーストリーム生成器は、ハードウェア・インプリメンテーションに、および極めてランダムで、長い周期、および実用上は予測不能なシーケンスを要求する様々なアプリケーションに特に好適である。

【0144】

第4の実施形態：

本発明の第4の実施形態によれば、上述の実施形態のうちの任意の1つによる疑似乱数生成器を使用して、暗号処理を行なうことができる装置が提供される。

【0145】

図11は、上記装置の一例を示す。本装置は、コンピュータシステムあるいはICモジュールのような情報処理装置で実現され得る。本装置は、例えば、上述の実施形態のうちの1つに従った疑似乱数生成器(P RNG) 1100、CPU 1101、I/Oインタフェース 1102、メモリ 1103、暗号プロセッサ 1104 およびバス 1105 を備えている。

【0146】

CPU 1101 は、暗号処理の制御、データ送信／受信、構成するユニット間でのデー

タ転送など、様々なオペレーションやプログラムを実行する。メモリ1103は、CPU1101によって実行されるプログラムおよび固定オペレーションパラメータを格納するROM、および、記憶エリアおよび／またはプログラムを実行したりパラメータの変更に使用されるワークエリアとして使用されるRAMを含んでいる。さらに、メモリ1103は、鍵データなどのようなセキュリティデータを格納するためにセキュア記憶領域を含んでいてもよいが、これは暗号の処理に必要である。改ざん防止(anti-tamper)構造を有するそのようなセキュア記憶領域を形成することは望ましい。

【0147】

暗号プロセッサ1104は、ストリーム暗号処理および／または解読処理のような暗号処理を行なう。また、暗号プロセッサ1104は、ROMに暗号処理プログラムを予め格納し、CPU1101にプログラムを読み取らせ実行させることにより実現してもよい。

【0148】

PRNG1100は、暗号処理用の鍵の生成に必要な擬似乱数を生成する。PRNG1100は、CAに基づくものであり、図3、6および10で示される構造のうちのいずれか1つであってもよい。

【0149】

I/Oインタフェース1102は、外部装置とのインタフェースをとり、例えば使用されるべき鍵を指定する情報の入力を受け、該鍵に基づいた暗号文データを出力する。また、I/Oインタフェース1102は、メディアリーダー／ライターまたはICモジュールのような外部装置または他の装置とデータ通信を行うデータ通信装置であってもよい。

【0150】

なお、添付のクレームあるいはその均等物の範囲内である限り、種々の変更、組み合わせ、下位組み合わせおよび変更が、設計必要条件および他の要因に依存して生じ得ることは、当業者に理解され得るものである。

【図面の簡単な説明】

【0151】

【図1】 2×Lセルオートマトンの一例を示す模式図である。

【図2】 二次元のセルオートマトン(2D-CA)の一例を示す模式図である。

【図3】 本発明の第1の実施形態による擬似乱数シーケンス生成器の構成例を示す模式図である。

【図4】 制御可能なセルオートマトン(CCA)のマクロブロック構成例を示す模式図である。

【図5】 図5(A)および図5(B)は、CCA中の要素の構成例を示す模式図である。

【図6】 本発明の第2の実施形態による擬似乱数シーケンス生成器の構成例を示す模式図である。

【図7】 本発明の第3の実施形態による、メモリを備えた非線形マッピングのブロックスキームである。

【図8】 本発明の第3の実施形態による、不均一な間引きのブロックスキームである。

【図9】 ラテン方格に基づいた非線形マッピングの典型的な形式を示す模式図である。

【図10】 本発明の第3の実施形態による擬似乱数シーケンス生成器の構成例を示す模式図である。

【図11】 本発明の第4の実施形態による暗号処理装置の構成例を示す模式図である。

【符号の説明】

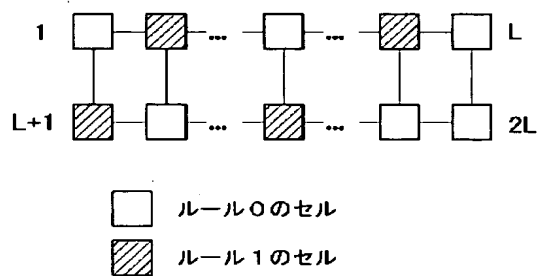
【0152】

310：二次元セルオートマトン

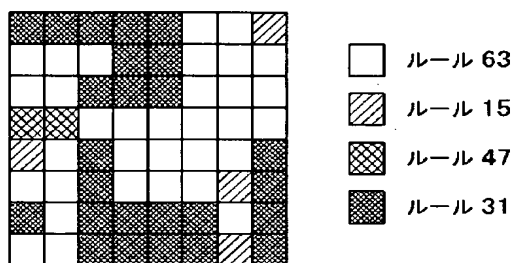
320：2×Lセルオートマトン

4 0 0 : 制御可能なセルオートマトン
7 0 1 ~ 7 0 3 : 非線形関数

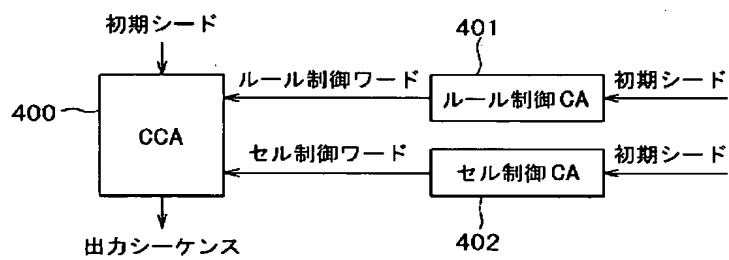
【書類名】 図面
【図 1】



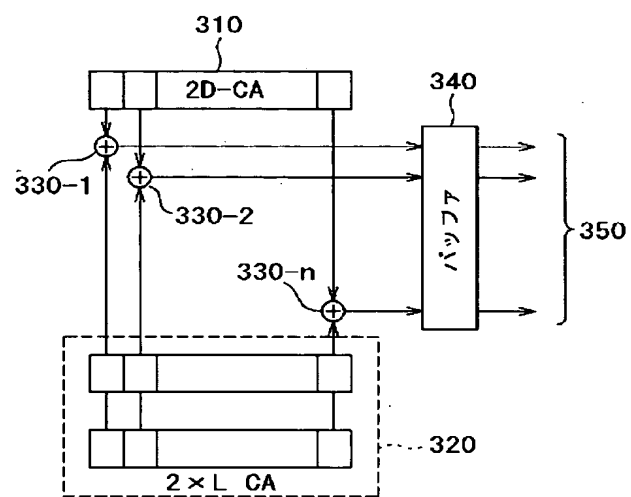
【図 2】



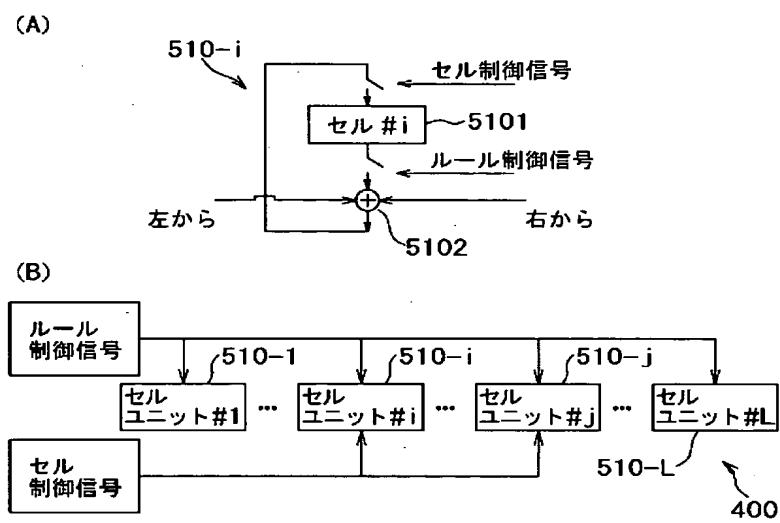
【図 3】



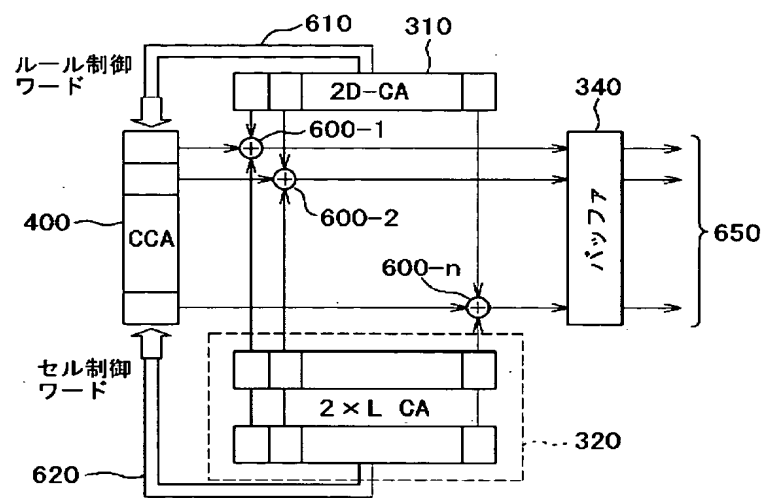
【図 4】



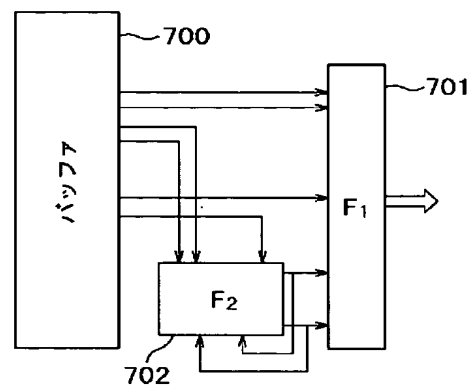
【図 5】



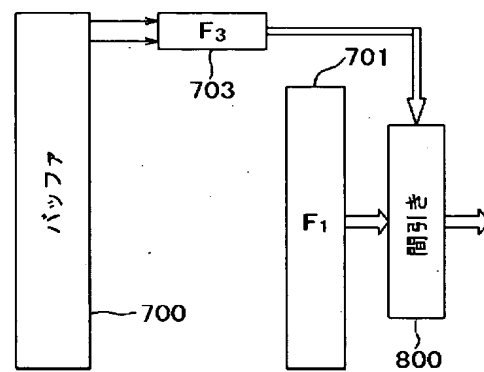
【図 6】



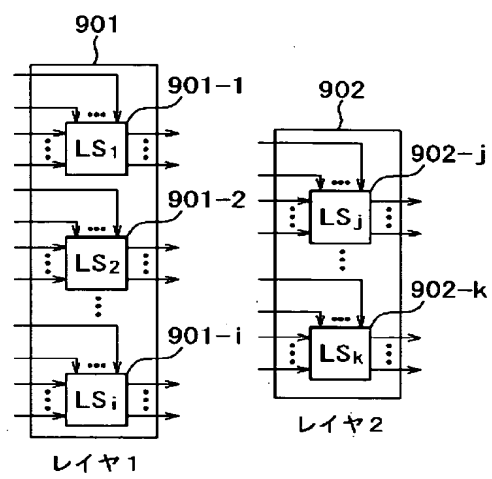
【図 7】



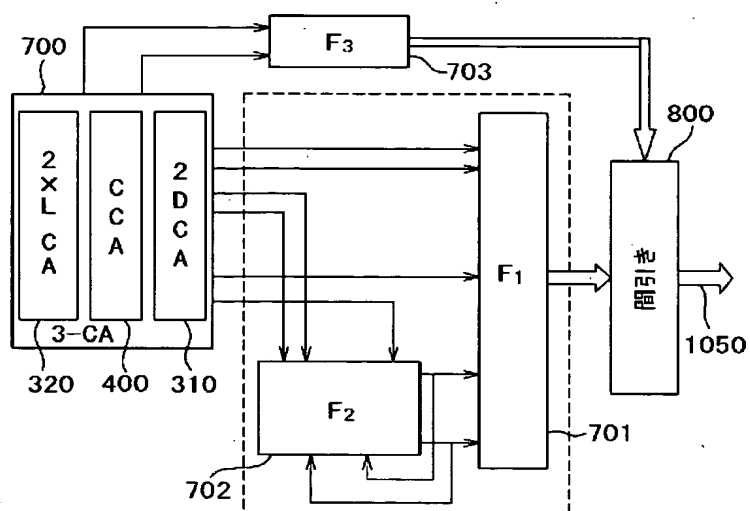
【図 8】



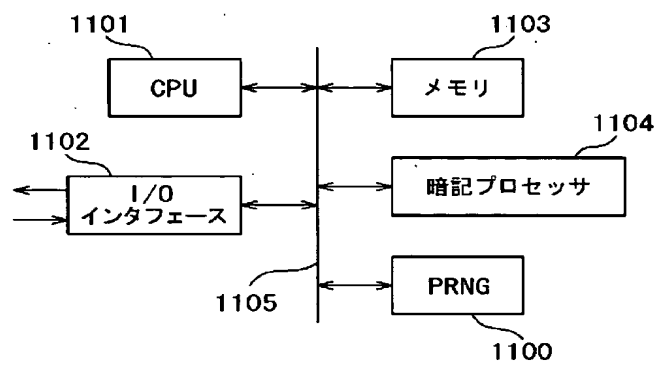
【図 9】



【図 10】



【図 11】



【書類名】 要約書

【要約】

【課題】 本発明の目的は、制御可能な周期を有する所望の擬似乱数シーケンスを生成するためのコンパクトな装置を提供することである。

【解決手段】 擬似乱数シーケンスを生成する装置は、第1のシーケンスを生成する二次元のセルオートマトン310、第2のシーケンスを生成する $2 \times L$ セルオートマトン320、第1のシーケンスおよび第2のシーケンスのビット対ビット $\text{mod } 2$ の和を得るための加算器330-1, 330-2, . . . , 330-n、および加算器330-1, 330-2, . . . , 330-nから結果として得られたシーケンスをバッファするためのバッファ340を備えている。

【選択図】 図3

出願人履歴

0 0 0 0 0 2 1 8 5

19900830

新規登録

5 9 7 0 6 2 9 9 3

東京都品川区北品川 6 丁目 7 番 3 5 号
ソニー株式会社